COMMONWEALTH OMBUDSMAN

# Uncovering the use of undercover powers

# 2022-23 Report to the Attorney-General on agencies' compliance with the *Crimes Act 1914*:

# Controlled Operations
# Delayed Notification Search Warrants
# Account Takeover Warrants

Report by the Commonwealth Ombudsman, Iain Anderson, under sections 15HO of Part IAB, 3ZZGH of Part IAAA and 3ZZVX of Part IAAC of the *Crimes Act 1914* (Cth)

November 2023

ISSN 2653-6498 - Print
ISSN 2653-6501 - Online





Commonwealth Ombudsman
Level 5, 14 Childers Street
Canberra ACT 2600
Tel: 1300 362 072
Email: ombudsman@ombudsman.gov.au

# Contents

# Our Report – At a glance

A controlled operation permits participants to engage in certain conduct that would otherwise be unlawful for the purpose of investigating a serious offence.

A delayed notification search warrant (DNSW) allows a covert search of premises to investigate certain terrorism offences, with the occupier of the premises being notified later.

An account takeover warrant (ATW) allows law enforcement to take control of an online account when investigating a serious offence.

## FINDINGS

We made no formal recommendations for remedial action.
We made 11 suggestions and 10 better practice suggestions:

- 7 suggestions and 5 better practice suggestions in relation to use of controlled operations
- 1 suggestion and 3 better practice suggestions in relation to use of DNSW powers
- 3 suggestions and 2 better practice suggestions in relation to use of ATW powers.

## KEY MESSAGES FROM THIS REPORT

- Agencies were generally compliant with legislative requirements in their use and administration of the controlled operations, DNSW and ATWs powers.
- The AFP do not frequently use DNSWs. The AFP need to improve their record keeping practices, particularly when sharing seized items or destroying data obtained under a DNSW.
- ATWs came into effect in September 2021 and have not been widely used.
- We continue to emphasise accurate and contemporaneous record keeping and for agencies to increase the capability of their staff who use the powers.

# Executive summary – what did we find?

This report presents the results of the Office of the Commonwealth Ombudsman's (the Office) inspections conducted under Part IAB (Controlled Operations) and Part IAAC (Account Takeover Warrants)of the *Crimes Act 1914*[1] (the Act) between 1 July 2022 and 30 June 2023, and Part IAAA (Delayed Notification Search Warrants) of the Act between 1 January 2023 and 30 June 2023.

## Controlled Operations

Under s 15HS of the Act, we inspected the Australian Commission for Law Enforcement Integrity (ACLEI) [2], the Australian Criminal Intelligence Commission (ACIC) and the Australian Federal Police's (AFP) use of controlled operations. A controlled operation under Part IAB of the Act permits authorised law enforcement and civilian participants to engage in certain conduct that would otherwise be unlawful for the purpose of investigating a serious Commonwealth offence.

Our inspections this year focused, in part, on assessing whether all conduct engaged in during a controlled operation, particularly by civilian participants, was explicitly controlled by an authority. In most instances, we found that the conduct of all 3 agencies during a controlled operations was compliant with the requirements of the Act. We have observed significant systemic improvement in the use and administration of controlled operations at both the AFP and the ACIC over the last 3 reporting periods, reflecting a greater level of maturity in their respective compliance cultures.

We identified some individual instances of non-compliance and related risks, namely an undisclosed conflict of interest with an urgent variation application, issues in reporting information in general registers, and risks of technical non-compliance with statutory procedures.

---

[1] https://www.legislation.gov.au/Series/C1914A00012.

[2] From 1 July 2023 ACLEI transitioned into the National Anti-Corruption Commission.

We are primarily concerned with officers having a comprehensive understanding of conducting controlled operations and keeping accurate records. This ensures both officers and participants have legal protection from prosecution for otherwise illegal acts. The controlled operation records are essential to the Ombudsman's inspections and reporting to ensure the confidence of the public and parliament that the agency is using these powers appropriately.

## Delayed Notification Search Warrants

The AFP is the only agency authorised to exercise a delayed notification search warrant (DNSW) under Part IAAA of the Act. A DNSW allows the AFP to conduct a covert search of premises (meaning a search the occupier is not aware of at the time) to investigate certain terrorism offences. The occupier of the premises is later notified of the search.

The DNSW power is not used frequently and no DNSWs were applied for or executed over both reporting periods. We are continuing to work with the AFP to improve record keeping and administrative practices, with a focus on capturing when information is shared and when decisions are made to destroy or retain information obtained using this power.

## Account Takeover Warrants

An account takeover warrant (ATW) under Part IAAC of the Act allows the AFP and the ACIC to take control of an online account when investigating a serious offence. Online accounts include social media accounts, online banking accounts and accounts associated with online forums.

Under s 3ZZVR of the Act we conduct inspections on an agency's use of ATWs to ensure they are exercising this power compliantly with Part IAAC of the Act. As part of our inspection activities, we also conduct 'health check' reviews on the compliance frameworks an agency has in place if they have not used the ATW powers over the records period. Over the inspection period we conducted one inspection of the AFP and one 'health check' of the ACIC.

The legislative framework for ATWs was enacted in September 2021 by the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth). Since enactment, the ACIC have not used any ATWs. We found the ACIC have governance and compliance frameworks in place to exercise powers under the Act compliantly.

The AFP had low usage of ATWs. We found they have good frameworks and controls in place to exercise powers under the Act compliantly, but there were still some areas for improvement. We noted many positives in our review of the AFP's frameworks and records, and in our process discussions with officers.

# Part 1. Oversight of Covert Law Enforcement Activities Under the Crimes Act 1914

## Introduction

The *Crimes Act 1914* (the Act) grants law enforcement agencies access to covert and intrusive powers with respect to the use of Controlled Operations, Delayed Notification Search Warrants and Account Takeover Warrants. The legislative requirements that allow law enforcement agencies to use these powers are found under Part IAB (Controlled Operations), Part IAAA (Delayed Notification Search Warrants) and Part IAAC (Account Takeover Warrants) of the Act.

Agencies that use powers under the Act must comply with reporting requirements and are overseen by the Commonwealth Ombudsman (our Office).

Our Office's oversight role is important for ensuring that agencies exercise these powers in accordance with legislative requirements and are accountable for instances of non-compliance. Our Office's reporting obligations provide transparency and a level of assurance to the Attorney-General and the public on the use of these powers.

This annual report provides a summary of the most significant findings regarding agencies' compliance with Part IAB, IAAA and IAAC of the Act from inspections conducted in the relevant period. We also report on matters that do not relate to specific instances of non-compliance, such as the adequacy of an agency's policies and procedures to demonstrate compliance with the Act.

### Part IAB of the Act – Controlled Operations

A controlled operation under Part IAB permits authorised law enforcement and civilian participants to engage in certain conduct that would otherwise be unlawful for the purpose of investigating a serious offence.

Under s 15HS of the Act, at least once every 12 months our Office must inspect the records of authorised agencies to determine the extent to which these agencies and their officers complied with Part IAB of the Act. This includes inspection of the use of the powers by the Australian Commission for Law Enforcement Integrity (ACLEI)[3], the Australian Criminal Intelligence Commission (ACIC) and the Australian Federal Police (AFP).

Additionally, our Office must inspect records of the ACIC to determine the extent of the ACIC's compliance with State controlled operations laws, unless the corresponding State controlled operations law provides for such an inspection, and only if the ACIC exercised those powers in the relevant period. The ACIC did not exercise these state powers in the period covered by this report.

Under s 15HO of the Act, our Office must report to the Attorney-General as soon as practicable after 30 June each year on inspections conducted during the preceding 12 months. In this report, the Ombudsman must include comments on the comprehensiveness and adequacy of the reports provided by agencies to the Attorney-General and our Office under ss 15HM and 15HN of the Act.

## Part IAAA of the Act – Delayed Notification Search Warrants

A delayed notification search warrant under Part IAAA allows the AFP to conduct a covert search of premises (meaning a search the occupier is not aware of at the time) to investigate certain terrorism offences. The occupier of the premises is notified of the search later.

Under s 3ZZGB of the Act, at least once in each 6-month period our Office must inspect the records of the AFP to determine the extent of the AFP's compliance with Part IAAA of the Act.

Under s 3ZZGH of the Act, as soon as practicable after each 6-month period our Office must present a report to the Attorney-General on the results of each inspection.

[3] From 1 July 2023 ACLEI transitioned into the National Anti-Corruption Commission.

### Part IAAC of the Act – Account Takeover Warrants

An account takeover warrant under Part IAAC allows law enforcement to take control of an online account when investigating a serious Commonwealth offence or a serious State offence that has a federal aspect. Online accounts include social media accounts, online banking accounts and accounts associated with online forums.

Section 3ZZVR of the Act requires our Office to annually inspect the records of the AFP and the ACIC to determine the extent of their compliance with Part IAAC of the Act.

Under 3ZZVX of the Act, the Ombudsman is required to provide a report to the Attorney-General at 12 monthly intervals with the results of each inspection.

## How we oversee agencies

Our Office uses a set of inspection methodologies and criteria that we apply consistently across each inspection. These are based on legislative requirements and administrative best practice standards. Further details on our inspection criteria are provided in **Appendix A** and **Appendix B**.

During the ATW reporting period we conducted a 'health check' review of the ACIC's ability to use account takeover warrants. A 'health check' assesses an agency's compliance framework and preparedness to use the account takeover warrant powers. Our criteria for this function is provided in **Appendix C**.

We assess an agency's compliance based on a risk-based selection of the agency's records, discussions with relevant agency staff, observations of agency policies and processes, and remedial action they have taken in response to issues we have previously identified.

Our Office takes a retrospective approach to inspecting an agency's use of powers. We generally inspect authorities or warrants that ceased to be in effect before the inspection. This retrospective approach seeks to minimise the risk associated with the sensitivity of ongoing operations. As a result, our 'inspection periods' (the period within which the inspection occurred) and our eligible 'records periods' (the period of time during which the records we are inspecting were made) differ.

Our inspections may identify a range of issues from minor administrative errors through to serious non-compliance that affects rights (notably privacy) or whether evidence was validly collected and systemic issues. If an issue is sufficiently serious or systemic, or was previously identified and not resolved, we may make formal 'recommendations' for remedial action. Where an issue of non-compliance is less serious or systemic, or was not identified before, we generally make 'suggestions' to address the non-compliance and to encourage agencies to take responsibility for identifying and implementing practical solutions. We may also make 'better practice suggestions' where we consider an agency's existing practice may expose it to compliance risks in the future.

For the next inspection year, 2023-24, our Office will no longer make better practice suggestions and will instead use recommendations, suggestions or make comment on issues or potential compliance risks.

To ensure procedural fairness and compliance with s 15HO(2) of the Act we provide agencies with a PDF copy of our post inspection report for comment on any perceived factual errors or any information which, if made public, could reasonably be expected to endanger a person's safety, prejudice an investigation or prosecution, or compromise law enforcement operational activities. The findings from our inspection reports and agency responses are desensitised and summarised to form the basis of our Office's annual report (this report) to the Attorney-General.

We follow up on any remedial action agencies have taken to address our findings at our next inspection.

# Part 2. Controlled Operations Inspections Activity

Part IAB of the Act enables law enforcement agencies to conduct controlled operations. Controlled operations are covert operations carried out, under internal authorisation, for the purpose of obtaining evidence that may lead to the prosecution of a person for a serious Commonwealth offence.

An appropriately authorised controlled operation provides legal protection for authorised law enforcement and civilian participants who engage in certain conduct during the operation that would otherwise be unlawful or lead to civil liability. Participants may engage in different types of conduct, so long as that conduct is directly authorised or appropriately related to authorised conduct. Examples of conduct could include possessing illicit goods, interfering with a consignment, or entering false data into a system.

Under Part IAB a controlled operation must not involve conduct that will seriously endanger the health or safety of any person; cause the death of, or serious injury to, any person; involve the commission of a sexual offence against any person; or result in significant loss of or serious damage to property (other than illicit goods).

To ensure an appropriate level of transparency about how and when controlled operations are used, Part IAB of the Act imposes several reporting obligations on agencies.

# Australian Commission for Law Enforcement Integrity

We conducted one inspection of the ACLEI's use of Part IAB powers between 7 and 11 November 2022. This inspection reviewed authorisations for controlled operations that expired or were cancelled between 1 July 2021 and 30 June 2022.

Table 1 – Summary of the ACLEI Controlled Operations records inspected between 7 and 11 November 2022

| Record type | Records made available | Records inspected |
|---|---|---|
| Urgent controlled operations authorities[4] | 0 | 0 |
| Formal controlled operations authorities[5] | 1 | 1 (100%) |
| **Total** controlled operations authorities | **1** | **1** |

## Progress since our last inspection

We reviewed the ACLEI's progress with implementing the suggestions and better practice suggestions arising from our 2020-21 inspection. While our 2021-22 inspection found the ACLEI had taken appropriate action to resolve all but one previous better practice suggestion, which related to improving quality assurance processes and guidance material, this outstanding item was resolved prior to this inspection.

[4] An authority granted, if the authorising officer is satisfied the delay caused by granting a formal authority may affect the success of the controlled operation.

[5] A formal controlled operation authority is granted by means of a written document, signed by the authorising officer.

## Findings from this inspection

Overall, we found that the ACLEI had good compliance with the requirements under Part IAB of the Act and sufficient controls in place to mitigate more serious risks of non-compliance. We found only low risk compliance and minor administrative matters during this inspection. These pertained to:

- administrative errors and insufficient governance of the general register for controlled operations activity
- authorised conduct performed under the authority was not recorded in the relevant controlled conduct record, and
- a record where a civilian participant was authorised to participate in the controlled operation, but it was not clear whether this occurred or a decision was made not to proceed.

We made one suggestion and one better practice suggestion which focused on improving quality assurance processes and correcting inaccurate records (being the controlled conduct record). Given the retrospective nature of our inspection, we acknowledged that accuracy and completeness of records coincided with the ACLEI not having yet implemented our previous better practice suggestion at the time of the non-compliance.

In response to our findings, the ACLEI confirmed a new register had been developed and relevant quality assurance checks were being commenced. The ACLEI had also reviewed and corrected the affected controlled conduct record.

## Comprehensiveness and adequacy of reports to our Office

The ACLEI submitted its 6-monthly reports under s 15HM of the Act for the periods 1 January 2022 to 30 June 2022 and 1 July 2022 to 31 December 2022, and its s 15HN of the Act 2021-22 annual report to our Office in accordance with the Act.

We inspected each of these reports and did not find any discrepancies. We consider the ACLEI has adequate processes in place to achieve compliance with the reporting requirements of Part IAB of the Act.

# Australian Criminal Intelligence Commission

We conducted one inspection of the ACIC's use of Part IAB powers between 26 and 30 June 2023. This inspection reviewed authorisations for controlled operations that expired or were cancelled between 1 July 2021 and 30 June 2022.

Table 2 – Summary of the ACIC Controlled Operations records inspected between 26 and 30 June 2023

| Record type | Records made available | Records inspected |
|---|---|---|
| Urgent controlled operations authorities | 0 | 0 (0%) |
| Formal controlled operations authorities | 32 | 27 (85%) |
| **Total** controlled operations authorities | **32** | **27 (85%)** |

The ACIC advised it did not use corresponding State or Territory controlled operations powers during the records period.

## Progress since our last inspection

We reviewed the ACIC's progress with implementing the suggestions and better practice suggestions arising from our 2021-22 inspection. We confirmed the ACIC took appropriate action in response to our previous inspection findings. The ACIC also disclosed minor discrepancies in their records which formed the basis of our previous findings, and we were satisfied with the remedial action in response to the compliance issues disclosed.

## Findings from this inspection

We found the ACIC had sufficient frameworks and quality control processes to use and administer the powers under Part IAB of the Act. The ACIC was responsive to our inspection requirements and proactively disclosed issues related to 2 records. The

issues we identified within the remaining records inspected were low risk or of a minor administrative error.

Our findings related to the 2 records disclosed by the ACIC and pertained to instances where the authority document did not particularise that the civilian participant conduct was 'under the direction of a law enforcement participant'.

While we made 2 findings related to these records, we were satisfied with the ACIC's identification, remediation, and disclosure of this issue. We did not make any suggestions or better practice suggestions, which is a decrease from the one suggestion and 2 better practice suggestions we made during our 2021-22 inspection.

## Comprehensiveness and adequacy of reports to our Office

The ACIC submitted its 6-monthly reports under s 15HM of the Act for the periods 1 January 2022 to 30 June 2022 and 1 July 2022 to 31 December 2022, and its s 15HN of the Act 2021-22 annual report to our Office in accordance with the Act.

We inspected each of these reports and did not find any discrepancies. We consider the ACIC has adequate processes in place to achieve compliance with the reporting requirements of Part IAB of the Act.

# Australian Federal Police

We conducted one inspection of the AFP's use of Part IAB powers between 17 and 21 April 2023. This inspection reviewed authorisations for controlled operations that expired or were cancelled between 1 January to 31 December 2022.

Table 3 – Summary of the AFP Controlled Operations records inspected between 17 and 21 April 2023

| Record type | Number of records made available | Number of records inspected |
|---|---|---|
| Formal controlled operations authorities | 34 | 20 (59%) |
| Urgent controlled operations authorities | 3 | 3 (100%) |
| **Total** Controlled Operation Authorities | **37** | **23 (62%)** |

## Progress since our last inspection

We reviewed the AFP's progress with implementing the 6 suggestions arising from our 2021-22 inspection. We considered the AFP have implemented all 6 suggestions and acknowledged the work undertaken by the AFP to improve compliance with Part IAB of the Act.

## Findings from this inspection

While the AFP had generally sound processes for using and administering the powers under Part IAB of the Act, we did identify some instances of non-compliance. The most serious of these included:

- not recording and appropriately managing a conflict of interest
- inadequate recording of civilian participants under an authority, and
- applicants and principal law enforcement officers (PLEO) having inconsistent understanding of their obligations and compliance requirements.

We made 6 suggestions and 4 better practice suggestions to the AFP. This represents an increase in the number of better practice suggestions from our previous 2021-22 inspection (during which we only made 6 suggestions).

### Conflict of interest within an urgent variation of authority record not recorded or managed

We identified a record where a pre-existing relationship between an applicant and Authorising Officer (AO) gave rise to what our Office would consider a conflict of interest.

While the AFP provided a further record in relation to the circumstances of the variation, there was no contemporaneous record of a declaration or acknowledgement of the conflict of interest. Additionally, given the circumstances surrounding the application and issuing of the urgent variation, there were no considerations recorded as to why the applicant or the AO could not have been changed to avoid any conflict of interest.

A failure to declare or sufficiently manage a conflict of interest is reportable misconduct under the AFP Commissioner's Order 2 on Professional Standards.

As a result, we made 3 suggestions in relation to this finding that:

- the AFP remind authorising officers about how to declare and manage any actual, potential, or perceived conflict of interest when assessing an application or exercising their power to issue or vary an authority
- the staff involved make a declaration of any actual, potential, or perceived conflict of interest in relation to authorising the urgent variation, and assess any impacts this conflict had on the issuing of the authority, and
- the AFP consider whether the actions in failing to declare and manage this conflict of interest is reportable misconduct pursuant to the Commissioner's Order 2 on Professional Standards.

In response to our findings, the AFP accepted our suggestions but disputed our assessment that the relationship amounted to a conflict of interest. The AFP's view was that there may have been a potential conflict of interest, but not an actual conflict of interest.

We remain of the opinion that the pre-existing relationship between the applicant and AO is of such a nature that a reasonable person would consider this to give rise to an apprehension of bias in the consideration of the application for the variation. This is particularly so in circumstances where options existed to prevent any real, potential, or perceived conflict in authorising the variation: it was not a situation where only that AO could consider the application.

### Inadequate recording of civilian participation in a controlled operations authority

The inspection identified one instance where a civilian participant listed in the final effectiveness report and conduct report was not listed in the application or authority.

We consider it important that the agency record whether a civilian participant's actions were authorised to support protection from unfairly being subjected to criminal or civil liability. Further, where there may be ambiguity in relation to conduct being performed by a civilian participant, the option carrying the least legal risk is to list them on the authority.

We suggested the AFP remind applicants for authorities to include all potential participants in the application and authority to conduct controlled operations in accordance with ss 15HA(2) and 15HB of the *Crimes Act 1914*.

In response, the AFP stated the records did not clearly reflect what occurred and that the civilian listed in the records did not engage in controlled conduct. They advised they would amend the final effectiveness report and participant conduct record for the authority to accurately reflect the participants and confirmed that no participants acted outside the parameters of the authority. The AFP advised they will continue to work to improve the accuracy and consistency of conduct records.

### Authorising and principal law enforcement officers' inconsistent understanding of their obligations or compliance responsibilities

We consider it best practice that any anticipated controlled conduct undertaken by law enforcement participants be explicitly included on an authorisation, particularly in circumstances where there is ambiguity in relation to conduct being performed by participants.

Through conversations with various AFP officers, we found there were different levels of understanding about what constituted ancillary conduct and what should be listed on

the authority and recorded in the Participant Conduct Record (PCR). These conversations also revealed inconsistent understanding of role-based obligations and compliance requirements when conducting a controlled operation.

We made one suggestion, that the AFP ensure training is provided on controlled operations to applicants and principal law enforcement officers. We also included 2 better practice suggestions for the AFP to update their guidance material to provide officers with consistent examples of ancillary conduct for inclusion in an authority and the PCR.

The AFP have accepted these suggestions and advised that they would consult internal training teams to ensure appropriate training is available for applicants and principal law enforcement officers to support compliance and best practice in the administration of controlled operations.

## Comprehensiveness and adequacy of reports to our Office

The AFP submitted its 6-monthly reports under s 15HM of the Act for the periods 1 January 2022 to 30 June 2022 and 1 July 2022 to 31 December 2022, and its s 15HN of the Act 2021-22 annual report to our Office in accordance with the Act.

We inspected each of these reports and identified potentially sensitive information in the AFP's annual reporting to the Minister. We suggested the AFP review this report to reconsider the inclusion of this information. This also included a better practice suggestion that the AFP review its internal guidance on disclosure of information. Both our suggestion and better practice suggestion were accepted.

# Part 3. Delayed Notification Search Warrants Inspections Activity

Part IAAA of the Act enables the AFP to apply for and execute delayed notification search warrants (DNSWs) to investigate terrorism offences punishable by imprisonment for 7 years or more. A DNSW allows a covert search of a premises, with the occupier of that premises being notified at a later time. Currently the AFP is the only prescribed agency that can apply for a DNSW.

From the commencement of Part IAAA of the Act in December 2014 up to December 2021, the AFP had not used this power. As a result, the focus of our inspections over these periods was to monitor the AFP's preparedness to use the powers compliantly with Part IAAA of the Act and ensure the AFP had developed appropriate governance frameworks to support compliance.

In March 2022 we conducted our first inspection of the AFP's use of DNSW powers as they advised they had executed 4 DNSW warrants over the 2020 to 2021 period. This was the first time the AFP had used DNSWs, and we did not observe any serious compliance issues, but noted improvements could be made to record keeping and internal guidance material.

## Australian Federal Police

We conducted one inspection of the AFP during 2022-23, from 13 to 16 June 2023. The inspection was for 2 records periods, 1 January 2022 to 30 June 2022 and 1 July 2022 to 31 December 2022.

On 23 June 2022, the AFP informed our Office there were no DNSWs applied for or executed during the period 1 January to 30 June 2022.

Even if the AFP has not used the powers, our Office still has an obligation to inspect under 3ZZGB. During our inspection, we confirmed the AFP advice that no DNSWs existed for either record period.

We made one suggestion and 3 better practice suggestions to the AFP. The AFP was responsive to our findings and advised our Office that it has fully or partially implemented suggestions, with a number of the partially implemented suggestions expected to be fully implemented by the end of the financial year.

## Progress since our previous inspection

We acknowledged the AFP's work and engagement with our Office in reviewing and updating all policy and procedural documentation in response to our previous reports. However, we noted delays implementing previous suggestions. We stressed such delays raise a potential risk of non-compliance and made further suggestions regarding governance and record-keeping documents.

## Inspection findings

As a result of our June 2023 inspection, in addition to the key findings detailed below, we made one suggestion and 3 better practice suggestions concerning low-risk or administrative matters such as record-keeping practices, procedures and guidance for sharing a thing seized under a DNSW, and ongoing demonstration to implement previous findings.

### Insufficient record of reasons not to destroy data

Section 3ZZCF(3) and 3ZZCG(3) of the Act requires data seized or moved under a DNSW to be destroyed by the Chief Officer if it is no longer or not likely to be required for a permitted purpose. Section 3ZZEA of the Act lists the purposes for which things may be used and shared.

During the inspection, the AFP advised that data seized under a previous DNSW was retained for court processes. The available record was not able to demonstrate where or when this decision was made.

To demonstrate compliance in future, we suggested the AFP ensure contemporaneous records demonstrate considerations to retain records under s 3ZZEA of the Act.

We further suggested the AFP update its National Guidelines to instruct users to record the reasons for the destruction by the Chief Officer (or their delegate) and fulfil their obligations under ss 3ZZEA, 3ZZCF(3) and 3ZZCG(3) of the Act.

### Need for clarification of when sharing of a seized thing may occur and what records must be made

Section 3ZZEA(5) of the Act states that an AFP officer may make a thing seized available to be used by another agency for a purpose mentioned in ss 3ZZEA(1), 3ZZEA(2) or 3ZZEA(3) of the Act and for a purpose listed under ss 3ZZEA(5)(c)-(f) of the Act.

We suggested the AFP clarify under what circumstances an item may be shared under s 3ZZEA of the Act, to inform its procedures for sharing a thing seized under a DNSW, and adapt its template and associated guidance accordingly to support officers to comply with their obligations under the Act when sharing seized things under a DNSW.

We made a better practice suggestion that the AFP update its guidance materials, specifically the DNSW Warrant Execution Booklet and DNSW Action Sheet to contain improved record keeping.

# Part 4. Account Takeover Warrants Inspections Activity

In September 2021, the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* added Part IAAC to the Act. Part IAAC of the Act allows the AFP and the ACIC to use an account takeover warrant to take control of a person's online account to gather evidence about a serious Commonwealth offence or a serious State or Territory offence that has a federal aspect.

The Act imposes requirements on the AFP and the ACIC when applying for and executing account takeover warrants. It also imposes requirements for how the AFP and the ACIC store and destroy protected information obtained through an account takeover warrant. The Act restricts the way these agencies use, communicate, or publish such information and requires them to keep records and provide reports about these covert activities.

## Australian Criminal Intelligence Commission

From 17 to 18 April 2023, we conducted an inspection of the ACIC's ATW policy, procedures, and guidance. The ACIC confirmed during pre-inspection correspondence that they had not used any ATWs during the inspection period. We confirmed this during the inspection. As a result, our inspection focused on assessing the policy and internal governance material the ACIC has in relation to ATWs and monitoring the implementation of our previous suggestions.

### Progress since our previous health check

From our previous 31 May 2022 to 2 June 2022 health check review of the ACIC's ATW policy, procedures, and guidance we made 3 better practice suggestions relating to ATWs to address areas for improvement.

The first better practice suggestion was for the ACIC to develop a definition of the term "material loss and damage" in relation to ATWs. During the inspection the ACIC advised

it had not finalised a position on the meaning of this term as it was awaiting advice from the AFP as to how they define the term so they could adopt a consistent position.

The second and third better practice suggestions were about the ACIC determining whether the ACIC can use an ATW to collect evidence in the absence of another warrant or power. During the inspection it was evident the ACIC had considered this issue, but had not yet finalised a position.

As the ACIC has not finalised its actions in relation to the previous better practice suggestions, we will continue to monitor their progress at future inspections.

# Australian Federal Police

From 6 March to 10 March 2023, we inspected the AFP's ATW records, policy, procedures, and guidance for the period 3 September 2021 to 30 June 2022. We reviewed records for 2 ATWs, assessed the AFP's progress against better practice suggestions from our previous health check, and provided compliance feedback to reduce the risk of future non-compliance by the AFP when using ATWs.

As a result of our inspection, we made 3 suggestions and 2 better practice suggestions. The suggestions related to retaining copies of applications for ATWs, ensuring that ATWs are revoked when no longer required, and appropriately recording communication of protected information.

## Progress since our previous inspection

Our first inspection of the AFP was conducted between 26 and 29 April 2022. As the AFP had not yet used the power, we inspected the AFP's operational readiness to use the ATWs by conducting a health check. This included reviewing the AFP's policy, procedures and guidance and undertaking discussion with compliance staff.

## Inspection findings

During our March 2023 inspection, we found the AFP had robust frameworks and controls in place to exercise ATW powers under the Crimes Act 1914 compliantly. In particular, we observed that:

- the AFP took satisfactory action to address the findings from our previous health check
- the AFP's affidavits for ATWs were comprehensive, and
- the AFP gave early consideration as to whether the target accounts would be restored following the execution of the account takeover warrant, and provided this advice to the issuing authority when applying for the ATW.

### Failure to keep a copy of each application for an account takeover warrant and potential sensitive material within the application

Section 3ZZVN of the Act requires the chief officer to keep a copy of each application for an ATW that was made by a law enforcement officer. While we were able to view a copy of the draft application relating to the 2 AFP ATWs, we could not locate a copy of the final signed application. The applicant advised us the issuing authority kept the sworn affidavit. We suggested the AFP seek and retain a copy of the sworn application for their 2 ATWs. We also suggested, as a matter of better practice, that the AFP update its governance and training to remind officers to seek and retain applications for ATWs.

The AFP advised they will seek a copy of the sworn applications and will update their Better Practice Guide and relevant governance to reinforce the expectation that officers seek and retain signed applications.

We also noted the ATWs may have contained child exploitation material within the application. It is unclear to us whether it is lawful for a magistrate or court to possess child exploitation material within Queensland. As a result, we suggested the AFP consider an approach to resolving this issue.

The AFP advised they are considering the issues raised in these findings.

### Delay in revoking warrant where ATW no longer required

We identified 2 ATWs that were executed and remained in force for a period longer than required due to the executing officer being on unplanned leave. In accordance with s 3ZZUU of the Act, these warrants should have been revoked when it was clear that the AFP no longer needed to take control of the target account under the warrant. The AFP generally has contingencies in place to adapt to situations where an executing officer is on unplanned leave to ensure warrants and other aspects of an operation can

progress appropriately. However, in this instance, we considered the time that had elapsed between the activity undertaken under the warrant and the time it was revoked to be unreasonably delayed.

We suggested the AFP ensure executing officers are aware of the requirement to immediately inform the chief officer when taking control of the target account is no longer required under an ATW, so that the warrant can be revoked.

In response to our suggestion, the AFP advised it will review their governance materials to ensure executing officers are aware of the requirement to immediately inform the chief officer when taking control of the target account is no longer required, so that the ATW can be revoked.

### Not recording the communication of protected information

The existence of an ATW is 'protected information', as defined in section 3ZZUK of the Act. We were advised the executing officer for the warrant disclosed the existence of the ATW to the account holder during the investigation, however the communication was not recorded in the Final Effectiveness Report and no Communication Form was completed. While we did not consider this an unauthorised disclosure of protected information, the disclosure of the protected information should have been recorded accurately.

We made a better practice suggestion the AFP consider developing guidance for circumstances where an ATW may be provided, or the existence of an ATW disclosed to relevant persons during the execution of the warrant. The AFP advised that they would review and update relevant governance material to include guidance on circumstances where an ATW may be provided, or the existence of an ATW disclosed, to relevant persons during the execution of the warrant. We will review progress against this better practice suggestion, and all other suggestions, at our next inspection.

# APPENDIX A – Inspection Criteria Controlled Operations

Objective: To determine the extent of compliance with Part IAB of the *Crimes Act 1914* (Part IAB) by the agency and its law enforcement officers (s 15HS(1))

## 1. Were controlled operations conducted in accordance with Part IAB of the Act?

### 1.1. Did the agency obtain the proper authority to conduct the controlled operation?

1.1.1. What are the agency's procedures to ensure that authorities, extensions, and variations are properly applied for and granted, and are they sufficient?

1.1.2. What are the agency's procedures for seeking variations from a nominated Tribunal member and are they sufficient?

1.1.3. What are the agency's procedures to ensure that ongoing controlled operations are subject to a nominated Tribunal member's oversight and are they sufficient?

1.1.4. What are the agency's procedures for cancelling authorities and are they sufficient?

### 1.2. Were activities relating to a controlled operation covered by an authority?

1.2.1. What are the agency's procedures to ensure that activities engaged in during a controlled operation are covered by an authority and are they sufficient?

1.2.2. What are the agency's procedures to ensure the safety of participants of controlled operations?

1.2.3. What are the agency's procedures for ensuring that conditions of authorities are adhered to?

## 2. Was the agency transparent and were reports properly made?

### 2.1. Were all records kept in accordance with Part IAB?

2.1.1. What are the agency's record keeping procedures and are they sufficient?

2.1.2. Does the agency keep an accurate general register?

### 2.2. Were reports properly made?

2.2.1. What are the agency's procedures for ensuring that it accurately reports to the Minister and Commonwealth Ombudsman and are they sufficient?

2.2.2. What are the agency's procedures for meeting its notification requirements and are they sufficient?

### 2.3. Was the agency cooperative and frank?

2.3.1. Does the agency have a culture of compliance? Was the agency proactive in identifying compliance issues? Did the agency self-disclose issues? Were issues identified at previous inspections addressed? Has the agency engaged with the Commonwealth Ombudsman's office, as necessary?

# APPENDIX B – Inspection Criteria Delayed Notification Search Warrants

Objective: To determine the extent of compliance with Part IAAA of the *Crimes Act 1914* by the Australian Federal Police and its eligible officers (s 3ZZGB)

## 1. Was an appropriate authority in place to exercise the delayed notification search powers?

### 1.1. Were applications for delayed notification search warrants properly made?

Process Checks

- What are the agency's procedures, controls, guidance, and training to ensure that delayed notification search warrants are properly applied for, and are they sufficient?
- Does the agency have procedures in place to ensure that warrants meet the requirements set out in ss 3ZZBE and 3ZZBF(5)–(9)?

Records Checks

We inspect applications, warrants and other agency records to assess whether:

- internal authorisation to apply for warrants was sought and given in accordance with ss 3ZZBA and 3ZZBB
- applications for warrants were made in accordance with Subdivisions A (normal process) and B (by electronic means) of Division 2 of Part IAAA
- the agency gave the eligible issuing officer sufficient information in the form of an affidavit for the officer to determine whether to issue a delayed notification search warrant under s 3ZZBD, and
- the agency complied with the requirements for applications by electronic means and associated record keeping obligations in s 3ZZBF.

### 1.2. Were applications for extensions of time to re-enter premises properly made?

Process Checks

- What are the agency's procedures, controls, guidance, and training to ensure that extensions of time to re-enter premises are properly applied for, and are they sufficient?

Records Checks

- We inspect applications, extensions, and other agency records to assess whether applications were made in accordance with s 3ZZCC and contained sufficient information for the eligible issuing officer to determine whether to grant the extension.

### 1.3. Were applications for extensions of time to examine or process things properly made?

Process Checks

- What are the agency's procedures, controls, guidance, and training to ensure that extensions of time to examine or process things moved from a warrant premises are properly applied for, and are they sufficient?

Records Checks

- We inspect applications, extensions, and other agency records to assess whether applications were made in accordance with s 3ZZCE and contained sufficient information for the eligible issuing officer to determine whether to grant the extension.

## 2. Were delayed notification search warrants properly executed?

Process Checks

- What are the agency's procedures to lawfully exercise entry, search and related powers, and are they sufficient?
- What are the agency's systems and/or records for capturing the exercise of powers, and are they sufficient?

Records Checks

We inspect records and reports relating to the exercise of warrant powers to assess whether:

- entry to premises was in accordance with section 3ZZCA and the warrant, including any conditions to which the warrant was subject
- the exercise of powers was in accordance with the warrant and ss 3ZZCA and 3ZZCB, and where applicable, extensions granted under s 3ZZCC (time to re-enter premises) and 3ZZCE (time to examine or process things moved from a warrant premises)
- assistance was provided and force was used in accordance with s 3ZZCD
- use and operation of equipment was in accordance with ss 3ZZCE, 3ZZCF, 3ZZCG and 3ZZCH, and
- compensation was paid for any damage to electronic equipment, data, or programs in accordance with s 3ZZCI.

## 3. Were notices to occupiers properly given?

Process Checks

- What are the agency's procedures, controls, guidance, and training to ensure that warrant premises occupier's notices are properly given, and are they sufficient?
- What are the agency's procedures, controls, guidance, and training to ensure that adjoining premises occupier's notices are properly given, and are they sufficient?
- What are the agency's procedures, controls, guidance, and training to ensure that extensions of time to give a notice are properly applied for, and are they sufficient?

Records Checks

We inspect notices, applications, extensions, and other records to assess whether:

- warrant premises occupier's notices were given in accordance with s 3ZZDA
- adjoining premises occupier's notices were given in accordance with s 3ZZDB
- warrant premises and adjoining premises occupier's notices were given within the timeframes required under the warrant and section 3ZZDC, and
- applications for an extension of time to give notice were made in accordance with s 3ZZDC and contained sufficient information for the eligible issuing officer to determine whether to grant the extension.

## 4. Did the agency properly manage things and data seized?

Process Checks

- What are the agency's procedures for managing things seized under a delayed notification search warrant, and are they sufficient?
- What are the agency's procedures for recording use, sharing, return and retention of things seized, and are they sufficient?
- What are the agency's procedures, controls, guidance, and training to ensure it meets its obligation to destroy copies and reproductions of data copied under a warrant, and are they sufficient?

Records Checks

We inspect records relating to the seizure, use, sharing, return and retention of things and data seized under delayed notification search warrants to assess whether:

- things were used and shared in accordance with s 3ZZEA
- things were returned in accordance with s 3ZZEB
- data was removed and copies of data were destroyed in accordance with ss 3ZZCF and 3ZZCG, and
- applications for orders about retention, forfeiture, sale, or disposal of things were made in accordance with s 3ZZEC and contained sufficient information for the eligible issuing officer to determine what order to make.

## 5. Has the agency satisfied its reporting and record-keeping obligations?

### 5.1. Were reports to the Minister and the Ombudsman properly made?

Process Checks

- What are the agency's reporting procedures, and are they sufficient?

Records Checks

- Have reports on each warrant been provided to the chief officer in accordance with s 3ZZFA?
- Did the chief officer report annually to the Minister in accordance with s 3ZZFB?
- Did the chief officer report 6-monthly to the Ombudsman in accordance with s 3ZZFC?

### 5.2. Were records properly kept?

Process Checks

- What are the agency's record keeping procedures, and are they sufficient?

Records Checks

- Did the agency keep documents connected with delayed notification search warrants in accordance with s 3ZZFD?
- Did the agency keep a register of delayed notification search warrants in accordance with s 3ZZFE?

## 6. Does the agency have a culture of compliance?

- Does the agency undertake regular training for officers exercising powers?
- Does the agency provide support and appropriate guidance material for officers exercising powers?
- Was the agency proactive in identifying compliance issues?
- Did the agency disclose compliance issues to the Commonwealth Ombudsman's Office?
- Were issues identified at previous inspections addressed?
- Has the agency engaged with the Commonwealth Ombudsman's Office as necessary?

# APPENDIX C – Inspection Criteria Account Takeover Warrants

Objective: To determine the extent of an agency's compliance with Part IAAC of the *Crimes Act 1914* (the Act) as it relates to the use of account takeover warrants.

## 1. Was appropriate authority in place for account takeover activities?

### 1.1. Did the agency have proper authority for account takeover activities?

Process Checks

- What are the agency's procedures to ensure that warrants, extensions, and variations are properly applied for, and are they sufficient?
- What are the agency's procedures to ensure that emergency authorisations are properly issued, and are they sufficient?

Records Checks

We inspect applications, warrants, authorisations, variations, and other agency records, to assess whether:

- applications for account takeover warrants were made in accordance with s 3ZZUN of the Act
- applications for account takeover warrants include accurate and sufficient information for the issuing authority to determine whether to issue the warrant under s 3ZZUP of the Act
- applications for extensions and/or variations to account takeover warrants were made in accordance with s 3ZZUS of the Act
- applications for account takeover emergency authorisations were made in accordance with Division 3 of Part IAAC of the Act, and
- account takeover warrants contained the information required by s 3ZZUQ of the Act.

### 1.2. Were account takeover warrants properly revoked and discontinued?

Process Checks

- What are the agency's procedures to ensure that warrants are properly revoked, and are they sufficient?
- What are the agency's procedures for ensuring that activity under a revoked warrant is discontinued, and are they sufficient?

Records Checks

We inspect agency records, to assess whether:

- account takeover warrants were revoked in accordance with s 3ZZUT of the Act, and discontinued in accordance with s 3ZZUU of the Act.

## 2. Were account takeover activities in accordance with the Act?

### 2.1. Were account takeover activities conducted in accordance with the authority of a warrant or emergency authorisation under the Act?[6]

Process Checks

- What are the agency's procedures for ensuring account takeover activity is conducted lawfully, and are they sufficient?
- Does the agency have an auditable and centralised system for managing account takeover activities?
- How does the agency demonstrate and provide assurance that the agency's systems and/or mechanisms for account takeover activities are in accordance with the Act and the terms of the warrant?
- What are the agency's procedures for ensuring warrant conditions are adhered to, and are they sufficient?

Records Checks

We assess the records and reports of account takeover activities against corresponding warrants and emergency authorisations, to assess whether:

- account takeover activity under an emergency authorisation was in accordance with s 3ZZUZ and s 3ZZUR of the Act
- account takeover activity under a warrant was in accordance with s 3ZZUR of the Act, including:
  - the warrant was executed in accordance with s 3ZZUR(5) of the Act – that is, execution did not include the doing of a thing that was likely to materially interfere with, interrupt or obstruct a communication in transit or lawful use of a computer by other persons (unless the doing of such things was necessary to do one or more of the things specified in the warrant), or caused material loss or damage to other persons lawfully using a computer
  - the warrant was executed in accordance with s 3ZZUR(8) of the Act – that is, the warrant was not executed in a way that caused loss or damage to data unless the damage is justified and proportionate, or resulted in a person's permanent loss of money, digital currency, or property (other than data)
- accounts, where applicable, were restored to the holder of the account once the warrant or emergency authorisation ceased, in accordance with s 3ZZUV or 3ZZVE of the Act, and
- assistance orders complied with s 3ZZVG of the Act.

---

[6] An account takeover warrant enables the action of taking control of the person's account (and doing specified things for the purpose of taking control of the account or anything reasonably incidental) and locking the person out of the account. Any other activities, such as accessing data on the account, gathering evidence, or performing undercover activities such as taking on a false identity, must be performed under a separate warrant or authorisation (p 6, Revised Explanatory Memorandum).

## 3. Is protected information collected under an account takeover warrant or emergency authorisation properly managed?

### 3.1. Was protected information collected under a warrant or emergency authorisation properly stored, used, and disclosed?

Process Checks

- What are the agency's procedures for securely storing protected information collected under a warrant or emergency authorisation, and are they sufficient?
- What are the agency's procedures for ensuring the proper use and disclosure of information, and are they sufficient?
- What are the agency's procedures for protecting privacy?

Records Checks

- We inspect the records and reports regarding use and disclosure of protected information required by the Act to assess whether the agency has used or disclosed protected information for a purpose other than one outlined in s 3ZZVH of the Act.

### 3.2. Was protected information retained or destroyed in accordance with the Act?

Process Checks

- What are the agency's procedures for ensuring that protected information is destroyed and/or retained in accordance with the Act, and are they sufficient?
- Does the agency regularly review its protected information to ensure compliance with the Act?

Records Checks

- We inspect the records relating to the review, retention and destruction of protected information, including records which indicate whether the chief officer was satisfied that protected information can be retained or destroyed (s 3ZZVJ of the Act).
- We inspect records to ensure all protected information collected under a warrant is destroyed as soon as practicable if not likely to be required for a listed purpose, or within 5 years of its creation, and within each period of 5 years thereafter unless the chief officer makes the decision to retain the information (s 3ZZVJ of the Act).

## 4. Did the agency comply with its record-keeping and reporting obligations?

### 4.1. Were all records kept in accordance with the Act?

Process Checks

- What are the agency's record keeping procedures, and are they sufficient?
- Does the agency maintain a register of applications for account takeover warrants and emergency authorisations that complies with s 3ZZVP and is it accurate?

Records Checks

- We inspect records to assess whether the agency met the record-keeping requirements under s 3ZZVN of the Act.
- We assess information contained in the original records against what is contained in the register to check whether the agency has met the requirements under s 3ZZVP of the Act.

### 4.2. Were reports properly made?

Process Checks

- What are the agency's procedures for ensuring that it accurately reports to the Attorney-General and the Commonwealth Ombudsman, and are they sufficient?

Records Checks

- We inspect copies of reports to assess whether the agency has met its reporting requirements under ss 3ZZVL and 3ZZVM of the Act. In conducting this assessment, we cross-check the information reported against corresponding original records.

## 5. Does the agency have a culture of compliance?

Process Checks

- Does the agency undertake regular training for officers exercising account takeover powers?
- Does the agency provide support and appropriate guidance material for officers exercising powers?
- Was the agency proactive in identifying compliance issues?
- Did the agency disclose compliance issues to the Commonwealth Ombudsman's office?
- Were issues identified at previous inspections addressed?
- Has the agency engaged with the Commonwealth Ombudsman's office as necessary?
- Does the agency have processes to ensure compliance, including:
    - quality control processes are supported by policy and practical guidance documents?
    - effective procedures to measure compliance and identify and action issues as they arise?
    - processes and training to identify and track issues that occur?
    - protocols for advising relevant officers of issues that arise?